

Homeland Security and Communications: A Compendium of Federal Programs

Prepared by:

Nancy J. Victory

Michael Lewis

Thomas S. Dombrowsky, Jr.

Catherine M. Hilke

August 2005



Wiley Rein & Fielding LLP

Introduction

The importance of communications in meeting homeland security needs of the United States is recognized in a large number of wide ranging federal programs and initiatives. This survey attempts to capture and categorize legislation pending before Congress, programs administered by the U.S. Department of Homeland Security, the role of the U.S. Department of Justice, activities arising before the Federal Communications Commission, and efforts at other government agencies and departments. The attached matrices reflect a best efforts attempt to provide a simple and timely overview of these complex, interrelated, and dynamic efforts.



About the Authors

ATTORNEYS AND CONSULTANTS

Nancy J. Victory
202.719.7344
nvictory@wrf.com

Ms. Victory is a partner in the Communications Practice and chair of the International Telecommunications Practice, where she advises a broad cross-section of the industry on the business implications of regulatory policy. Previously she served as Assistant Secretary of Commerce for Communications and Information and Administrator of the National Telecommunications and Information Administration under President Bush. Ms. Victory has also been named Chair of the FCC Advisory Committee for the 2007 World Radiocommunication Conference. She received her J.D., *cum laude* from the Georgetown University Law Center.

Michael Lewis
202.719.7338
mlewis@wrf.com

Mr. Lewis is an engineering consultant in the Communication Practice, where he is actively involved in a variety of public safety issues including interference to 800 MHz public safety operations, public safety spectrum allocations in the 700 MHz and 4.9 GHz bands and has extensive experience in interpreting Part 90 of the FCC's rules in general. He previously held several engineering positions within the FCC, including engineering advisor to the Chief of the FCC's Private Radio Bureau. Mr. Lewis received his B.S. in Electrical Engineering from the University of Michigan.

Thomas S. Dombrowsky, Jr.
202.719.7236
tdombrowsky@wrf.com

Mr. Dombrowsky is an engineering consultant in the Communications Practice, where he advises on wireless technology and licensing matters, particularly involving mobile radio and microwave communications. Previously he served as chief of the Licensing and Technical Analysis and Broadband Branches of the FCC's Wireless Telecommunications Bureau and as an engineer in the Wireless Telecommunications and Private Radio Bureaus. He received his B.S. in Electrical Engineering from Lehigh University.

Catherine M. Hilke
202.719.7418
chilke@wrf.com

Ms. Hilke is an associate in the Communications Practice, where she is engaged in a wide variety of regulatory issues affecting the wireless industry. She received her J.D., *magna cum laude* from the Columbus School of Law, The Catholic University of America.

SUMMER ASSOCIATES

Marjorie B. Manne

Ms. Manne was a 2005 summer associate at WRF. She is a J.D. candidate at the George Mason University School of Law.

Steven E. Merlis

Mr. Merlis was a 2005 summer associate at WRF. He is a J.D. candidate at Northwestern University School of Law.

Stephen S. Neuman

Mr. Neuman was 2005 summer associate at WRF. He is a J.D. candidate at the Washington University School of Law.



Table of Contents

	Page
Section 1: Department of Homeland Security	1
Section 2: Department of Justice	12
Section 3: Federal Communications Commission	15
Section 4: Department of Commerce	32
Section 5: Department of Agriculture	33
Section 6: Department of Health and Human Services	34
Section 7: Congress	36



U.S. Department of Homeland Security

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Project SAFECOM— Generally	<p>SAFECOM serves as an umbrella program within the Federal government—it oversees all initiatives and projects pertaining to public safety communications and interoperability.</p> <p>SAFECOM's goal is to allow public safety agencies and first responders to talk across disciplines and jurisdictions (Federal, state, local) via wireless radio communications systems, exchanging voice and/or data with one another on demand, in real time.</p> <p>SAFECOM's optimal public safety radio communications system would include: dedicated channels and priority access that is available at all times to handle unexpected emergencies; reliable one-to-many broadcast capability; highly reliable and redundant networks that are engineered to withstand natural disasters and other emergencies; the best possible coverage within a given geographic area, with a minimum of dead zones; and, unique equipment designed for quick response in emergency situations.</p>	<p>SAFECOM is organizing a broad communications interoperability effort between first responders across the country.</p> <p>Discussed in the next three sections of this chart are SAFECOM's most recent projects.</p>	<p>The Office of Management and Budget established Project SAFECOM in October 2001. SAFECOM is managed by the DHS Science and Technology (S&T) Directorate's Office for Interoperability and Compatibility (OIC).</p> <p>SAFECOM serves over 50,000 local and state agencies and 100 Federal agencies.</p> <p>SAFECOM estimates that full interoperability could take 20 years.</p> <p>The 9/11 Commission recommended significant funding increases to help with communications between public safety agencies.</p>



INTEROPERABILITY (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
RapidCom 9/30 (SAFECOM Initiative)	<p>Interoperability initiative for 10 high-risk urban areas. (New York, Chicago, Washington, DC and the surrounding Capital Region, Los Angeles, San Francisco, Philadelphia, Houston, Jersey City, Miami, and Boston).</p> <p>At the incident area, RapidCom helps first responders from various disciplines and jurisdictions communicate through existing equipment that is made interoperable by a patch-panel device that interconnects various models of equipment.</p> <p>RapidCom's additional assistance includes: technical help in setting up the technology; development of Standard Operating Procedures (SOP) that guide all public safety officials; training in the use of the equipment; help in conducting test exercises; and assistance in establishing a regional governance structure that brings all relevant agencies together.</p>	RapidCom is intended to enable communication between public safety workers in these urban areas to communicate both internally and with those in other urban areas following an emergency incident.	<p>President Bush initially announced the program in July 2004, with completion scheduled for Sept. 30, 2004.</p> <p>The RapidCom initiative concluded with the Urban Area Summit, held on October 27th and 28th, 2004, in Washington, DC.</p> <p>At this meeting, public safety practitioners from the ten RapidCom urban areas shared best practices, lessons learned, and other experiences resulting from this initiative.</p>
Statewide Communications Interoperability Planning (SCIP) Methodology (SAFECOM Initiative)	<p>The SCIP Methodology outlines ten essential planning phases that states should use to create their own statewide communications interoperability plans.</p> <p>The phases include: 1) establishing key relationships and funding; 2) gathering information; 3) creating a project plan and roadmap; 4) identifying roles and responsibilities for the project team; 5) recruiting focus group participants and meeting preparation; 6) conducting focus group interviews; 7) analyzing data and preparing for strategic planning sessions; 8) conducting strategic planning sessions; 9) developing a statewide communications interoperability strategic plan; and 10) developing guidelines for the first 90 days of implementation.</p>	Given that 90% of the communications infrastructure is owned and maintained at a local or state level, the SCIP methodology was designed and implemented with the needs of state and local agencies in mind.	<p>SAFECOM and the OIC announced the SCIP Methodology on January 26, 2005.</p> <p>DHS designed the SCIP Methodology based on Virginia's plan to establish statewide interoperability.</p>



INTEROPERABILITY (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
Statement of Requirements (SoR) for Wireless Public Safety Communications and Interoperability (SAFECOM Initiative)	<p>The SoR proposes functional requirements (including technical requirements and business models for interoperability implementation) for communications interoperability in day-to-day, task force, and mutual aid operations.</p> <p>Specifically, the SoR focuses on the functional needs of public safety first responders—EMS personnel, firefighters, and law enforcement officers—to communicate and share information. The communications mode may be voice, data, image, video, or multimedia.</p>	<p>SAFECOM intended the SoR to serve as a first step toward establishing base-level interoperability standards for all public safety agencies.</p> <p>The SoR was also intended to assist private industry with prioritizing its research and development strategies in-line with the communications needs of the public safety community.</p>	<p>Released April 2004.</p> <p>SoR proposes some interoperability requirements that extend through 2019.</p> <p>The SoR was created using a “bottom-up” approach, seeking input from local entities.</p> <p>Over a period of nine months, SAFECOM gathered representatives from law enforcement, fire, and EMS organizations to discuss interoperability requirements. SAFECOM worked with National Institute of Justice’s CommTech staff to draft the SoR, which was submitted to a National Public Safety Telecommunications Council working group for technical review and endorsement. It was finally provided to 55 regional planning committees for comment before final review and release.</p>



INTEROPERABILITY (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
Intelligence Reform and Terrorism Prevention Act of 2004	<p>Requires DHS, in consultation with the FCC and the National Telecommunications and Information Administration (NTIA), to conduct a study on strategies that meet public safety telecommunications needs, including:</p> <ol style="list-style-type: none">1) the need and efficacy of deploying nationwide interoperable communications networks;2) the capacity of public safety entities to utilize wireless broadband applications; and3) the communications capabilities of all emergency response providers, including hospitals and health care workers, and current efforts to promote communications coordination and training among emergency response providers.	The DHS must seek input from Federal, State, local, and regional emergency response providers regarding the operation of a potential nationwide interoperable broadband mobile communications network.	The DHS must report its findings to Congress by December 17, 2005.
Presidential Determination: Improving Spectrum Management for the 21st Century	<p>The Determination directs DHS to:</p> <ol style="list-style-type: none">1) Identify the public safety spectrum needs of the public safety community; State, local, tribal, and regional governments; and the private sector. DHS should consult with the FCC and the Department of Commerce. (DOC) (Due May 30, 2005).2) Develop a Spectrum Needs Plan that addresses issues related to spectrum use by the public safety community. DHS should consult with various Federal agencies and departments, including the FCC and the DOC. (Due November 30, 2005).	This Determination requires DHS to evaluate how to distribute and use spectrum for public safety purposes.	<p>The Determination was released November 30, 2004.</p> <p>DHS will submit the Spectrum Needs Plan to the President.</p>



NETWORK SECURITY AND RELIABILITY

Initiative	Description	Relevance to Communications	Status/Notes
Telecommunications Service Priority (TSP) TSP is provided by the NCS.	<p>The TSP program provides the framework for the priority restoration and provisioning of any qualified national security and emergency preparedness (NSEP) telecommunications services.</p> <p>NSEP services are those services used to maintain a state of readiness or manage any emergency (local, national, or international) that harms the population, damages property, or threatens the NSEP posture of the U.S.</p> <p>A restoration priority is assigned to new or existing telecommunications services to ensure restoration before non-TSP services. Priority restoration should be assigned to a new service when interruptions may have a serious, adverse effect on the supported NSEP function.</p> <p>A provisioning priority facilitates priority installation of new telecommunications services. Provisioning on a priority basis becomes necessary when a service user has an urgent requirement for a new NSEP service that must be installed quickly.</p>	The TSP Program rules authorize priority treatment to the following telecommunications services: common carrier services that are interstate and foreign telecommunications services; common carrier services that are intrastate telecommunications services inseparable from interstate or foreign telecommunications services; and services that are provided by government and non-common carriers and are interconnected to common carrier services assigned TSP priority levels.	In 1988, the FCC issued a Report and Order (FCC 88-341) establishing the TSP Program.



NETWORK SECURITY AND RELIABILITY (cont.)

Initiative	Description	Relevance to Communications	Status/Notes
National Response Plan (particularly Emergency Service Function # 2—Telecommunications)	<p>The National Response Plan (NRP) is a plan designed to handle domestic emergencies. Part of the NRP outlines 15 Emergency Service Functions (ESFs) that structure how support will be provided to protect and restore critical infrastructure during an emergency.</p> <p>ESF # 2 (telecommunications) coordinates Federal actions to restore the telecommunications infrastructure and provide necessary NSEP communications.</p> <p>The National Coordinating Center for Telecommunications (NCC)—the operational component of the DHS/IAIP/NCS—is the headquarters for ESF # 2 operations. The NCC staff assesses anticipated/actual damage, identifies NSEP service requirements, prioritizes requirements, monitors the developing situation/response, produces status reports, and coordinates service provisioning and restoration as required.</p> <p>ESF # 2 also relies on GETS, WPS, TSP, and the Shared Resources High Frequency Radio Program (SHARES) to help with communications support in the event of an emergency.</p>	<p>The NRP and ESF # 2 make the protection and restoration of the telecommunications infrastructure a priority for the DHS (NCC).</p>	<p>The NRP was released in December 2004.</p> <p>ESF # 2 supplements the provisions of the National Plan for Telecommunications Support in Non-Wartime Emergencies.</p> <p>DHS will activate ESF # 2 based on staff reports and advice from local and state agencies. The NCC staff also receives information and advice from industry representatives.</p> <p>Supporting Federal agencies under ESF # 2 include the FCC, USDA/FS, DOC, DOD, DOI, and GSA.</p> <p>The FCC also is a supporting agency under ESF # 5 (Emergency Management) and ESF # 15 (External Affairs).</p>



NETWORK SECURITY AND RELIABILITY (cont.)

Initiative	Description	Relevance to Communications	Status/Notes
Communications Resource Information Sharing (CRIS) NCS manages CRIS.	<p>The CRIS initiative establishes an information source that identifies transportable communications equipment, over-the-counter services, and fixed communications networks of the Federal government that could be used on a shared basis with other Federal organizations to support NSEP requirements.</p> <p>CRIS is open to all NCS member organizations (23 Federal departments and agencies) and their affiliates on a voluntary basis. Identification of telecommunications resources for use in CRIS is also on a voluntary basis, and the sharing of such resources is not to interfere with an organization's mission.</p>	CRIS reinforces the federal communications infrastructure by facilitating the shared use of communication assets, services, and capabilities during an emergency.	<p>The Executive Office of the President approved CRIS in February 1996.</p> <p>The NCS CRIS Working Group guides the CRIS initiative. The Chief, Operations Division (N3), NCS provides day-to-day administration of CRIS.</p> <p>Twenty-six Federal and industry organizations contribute resources to CRIS.</p>
The recent creation within DHS of the Assistant Secretary for Cyber Security and Telecommunications	The individual in this position will be responsible for identifying the vulnerability of critical telecommunications infrastructure, providing threat information, and leading the national response to attacks on telecommunications.		<p>Position announced in July 2005. No individual nominated.</p> <p>The Assistant Secretary will report to the Undersecretary for Preparedness, who reports directly to the DHS Secretary.</p> <p>The previous position charged with communication-security duties was five steps below the DHS Secretary.</p>



PRIORITY ACCESS			
Initiative	Description	Relevance to Communications	Status/Notes
<p>Government Emergency Telecommunications Service (GETS)</p> <p>GETS is provided by The National Communications System (NCS), which was transferred to DHS on March 1, 2003.</p>	<p>Provides NSEP users with emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN) when their normal telecommunications means are unavailable or congested during an emergency.</p> <p>GETS calls receive priority treatment through enhanced routing, controls such as trunk queuing, trunk sub-grouping, and trunk reservation, and through exemption from restrictive network management controls used to reduce network congestion.</p> <p>GETS is accessed through a universal access number and Personal Identification Number (PIN) card. Once the caller is authenticated, his or her call receives priority treatment.</p>	<p>GETS uses the networks controlled by the following entities: local networks from LECs and wireless providers, long-distance networks from IXC's (AT&T, MCI, and Sprint), and government leased networks (Federal Technology Service and the Defense Switched Network).</p>	<p>The President directed the Office of the Manager, NCS (OMNCS) to develop GETS.</p> <p>On 9/11, 18,000 GETS calls were made (10,000 in NY and DC), and the call completion rate exceeded 95%. During the 2001 Nisqually Earthquake near Seattle, there were 400 successful GETS calls.</p>



EMERGENCY ALERT			
Initiative	Description	Relevance to Communications	Status/Notes
Homeland Security Advisory System (includes Threat Advisories, Information Bulletins, and a color-coded Threat Level System)	<p>The DHS distributes Threat Advisories and Information Bulletins to Federal, state, and local governments, private sector organizations, and international partners.</p> <p>Threat Advisories contain actionable information about a threat targeting critical national infrastructures or key assets.</p> <p>Information Bulletins communicate information that does not meet the timeliness, specificity, or significance thresholds of Threat Advisories.</p> <p>The Threat Level System is the widely recognizable color-coded system used to communicate threat levels with public safety officials and the public, so protective measures can be implemented to reduce the likelihood or impact of an attack.</p>	The Advisory System communicates threat information and vulnerability assessments to public safety officials, private entities, and the public.	<p>In March 2002, President Bush issued Homeland Security Presidential Directive-3, establishing the Homeland Security Advisory System.</p> <p>The DHS is responsible for operating the Advisory System.</p>
Digital Emergency Alert System (DEAS) National Capital Region Pilot	Over the past year, the Federal Emergency Management Agency (FEMA) and the Information Analysis and Infrastructure Protection (IAIP) Directorate (both part of DHS), along with the Association of Public Television Stations (APTS), conducted a pilot project throughout the DC metropolitan area to demonstrate how DHS can improve public warnings during emergencies through the use of local public television digital broadcasts.	DHS also relied on commercial and public television and radio broadcasters, cell phone service providers, satellite radio, cable and Internet providers, and equipment manufacturers to develop a foundation for deploying DEAS.	<p>DHS launched the DEAS National Capital Region Pilot on October 21, 2004.</p> <p>DHS recently extended the DEAS project for six months. The second phase of this project will focus more on establishing a national DEAS.</p> <p>DEAS will supplement the existing national Emergency Alert System.</p> <p>Private industry participants include Cingular, T-Mobile, Nextel, USA Mobility, CTIA, Comcast, NCTA, WTOP (AM) Washington, WRC-TV Washington, and XM Satellite Radio.</p>



EMERGENCY ALERT (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
Shared Resources High Frequency Radio Program (SHARES) SHARES is provided through NCC.	<p>SHARES brings together existing HF radio resources of federal, state, and industry organizations to provide a single, interagency emergency message handling system for Federal departments and agencies.</p> <p>Certain conditions must exist to use SHARES, including: the information must support NSEP requirements; the information must be communicated to a Federal entity and be of critical importance to the Federal government, the entity's mission, and/or involve the preservation of life and property; the primary means of communications must be inoperative or unavailable for use; and the processing of SHARES message traffic must not interfere with the primary mission requirements of the SHARES participants.</p> <p>To access SHARES, a user contacts the nearest SHARES station listed in the SHARES Directory and requests assistance in processing a SHARES message.</p> <p>SHARES is available on a 24-hour basis.</p>	<p>As of July 2004, over 1000 HF radio stations, representing 93 Federal, state, and industry entities were resource contributors to SHARES.</p> <p>Over 150 HF frequencies have been authorized for use in SHARES.</p>	<p>SHARES further implements Executive Order No. 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," dated April 3, 1984.</p> <p>The SHARES HF Interoperability Working Group (IWG) provides guidance for the SHARES radio network.</p> <p>The Manager, NCC, is responsible for day-to-day operations.</p> <p>SHARES stations are located in every state and at 20 overseas locations.</p> <p>194 emergency planning and response personnel participate.</p> <p>A SHARES Bulletin is published periodically to keep members updated on program activities.</p>



TECHNOLOGY DEVELOPMENTS			
Initiative	Description	Relevance to Communications	Status/Notes
Radio Frequency Identification Device (RFID) Testing	<p>DHS plans to use RFIDs within its United States Visitor and Immigrant Status Indicator Technology (US-VISIT) border control program to support an automated biometrically enabled entry-exit border operation.</p> <p>DHS is experimenting with RFIDs to track the path of baggage and ground vehicles throughout airports and to ensure that only authorized airport personnel access ground vehicles.</p>	RFIDs use radio frequency waves to transfer data between a movable object and a reader. RFIDs can be used to identify, track, and locate people and objects.	<p>DHS (US-VISIT) hopes to begin testing RFID technology at ports in Arizona, New York, and Washington state by July 31, 2005 (testing is expected to continue through Spring 2006).</p> <p>The Airport Access Control Pilot Program (sponsored by the TSA—part of DHS) funds the experimental use of RFID technology to enhance airport security. Recently, the TSA awarded 10 airports a total of \$8.2 million in grants.</p> <p>The 9/11 Commission supports RFID technology. However, Senators Burns and Leahy and a GAO report have expressed privacy and security concerns about the use of RFIDs.</p>



U.S. Department of Justice

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Integrated Wireless Network (IWN)	IWN is a joint effort by the DOJ, DHS, and the Treasury to provide a consolidated nationwide federal wireless communications service that replaces stand alone component systems and supports first responders and law enforcement with integrated communications services (voice, data, and multimedia).	IWN will implement solutions to provide federal agency interoperability with appropriate links to state, local, and tribal public safety and homeland security entities.	<p>The IWN partnership began in October 2001. IWN is governed by the IWN Executive Board, which is comprised of the CIOs from DOJ, DHS, and Treasury.</p> <p>As of January 2005, five companies were in the running to develop IWN—AT&T, Boeing, General Dynamics, Lockheed Martin, and Motorola.</p> <p>The government estimates that IWN should take between 5-10 years to complete. The estimated funding for IWN is \$2.5 billion (however, the ceiling is \$10 billion).</p> <p>The government estimates that IWN will serve over 80,000 law enforcement users and will operate through 2,500 sites.</p> <p>An IWN pilot is being tested in Seattle, Washington. It is based on earlier IWN architecture completed in August 2002 (Project 25 compatible, VHF trunked land mobile radio, IP backbone). The pilot went operational in 2004.</p>



INTEROPERABILITY (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
High Risk Metropolitan Assistance Project: The 25 Cities Project	<p>Interoperability initiative for 25 high-risk metropolitan areas: Atlanta, Baltimore, Boston, Charlotte, Chicago, Dallas, Denver, Detroit, Hampton Roads/Norfolk, Honolulu, Houston, Jacksonville, Los Angeles, Miami, New Orleans, New York, Philadelphia, Phoenix, Portland, San Diego, San Francisco, Seattle, St. Louis, Tampa, and Washington DC.</p> <p>The Project consists of five phases: 1) identify vulnerable cities; 2) meet with local personnel, collect key requirements; 3) evaluate existing communications capabilities, prioritize requirements, recommend solutions to participating agencies; 4) develop plans for installing new equipment and leveraging existing resources; 5) procure and install equipment, implement new operational procedures.</p>	Provides federal law enforcement/homeland security agencies and local authorities with basic inter-system communication abilities during emergency situations.	<p>Managed by the DOJ's Wireless Management Office (WMO).</p> <p>The 25 Cities Project conducted real-life exercises in New York (July 2004) and Seattle (January 2005) to test recently implemented interoperability solutions.</p> <p>The Project has integrated some of its efforts into the broader IWN initiative.</p>



INTEROPERABILITY (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
CommTech Program	<p>CommTech is a comprehensive interoperability project targeted at state and local law enforcement agencies.</p> <p>CommTech is developing open architecture standards for voice, data, image, and video communications systems. These standards will help users exchange information among fixed facilities, mobile platforms, and personal devices.</p> <p>CommTech also researches, develops, tests and evaluates technology solutions that facilitate interoperability. Areas of interest include VoIP; standards-based radios/systems; cognitive radio; software-defined radio; wireless broadband data communications; antenna research; in-building coverage; multi-band radio; and network coverage extension for rural environments.</p>	CommTech facilitates communications interoperability among state and local law enforcement agencies.	<p>Operated through the DOJ's National Institute of Justice (NIJ).</p> <p>The interoperability standards that CommTech ultimately develops will be incorporated into a Strategic Plan that law enforcement agencies can use to achieve interoperability.</p> <p>NIJ funds communications technology research and development through directed solicitations. The FY 2005 Communications Technology solicitation has closed and applications are under review.</p> <p>CommTech is currently assisting Maryland, Virginia, and Washington DC to develop the Capital Wireless Integrated Network—the first multi-state, inter-jurisdictional public safety integrated wireless network.</p>
Community Oriented Policing Service (COPS) Interoperable Communications Technology Program	<p>The Program awards technology grants to law enforcement for the purpose of enhancing wireless voice and data interoperability.</p> <p>The Program supports regional, multi-jurisdictional, and a limited number of federal interoperability projects.</p>	Aids in the research and development of technology for communications interoperability.	<p>Managed through the DOJ's COPS program.</p> <p>COPS was appropriated \$90 million in FY 2005 for this program. It expects to fund 25-30 jurisdictions. COPS awarded \$82.6 million to 23 jurisdictions in 2004.</p>



Federal Communications Commission

INTEROPERABILITY			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
700 MHz WT Dkt. No. 96-86	In 1998, the FCC designated approximately 10 percent of the 700 MHz public safety allocation (2.6 MHz) for interoperable communications. Since that time, the FCC has developed technical standards and frequency coordination and licensing procedures designed to promote the most efficient and effective use of this spectrum.	Interoperability is the ability of different governmental agencies to communicate with each other and across jurisdictions. Such interoperability is designed to promote safety of life and property through seamless, coordinated communications on the interoperability spectrum.	The FCC established technical standards for both narrowband and wideband use of the channels reserved for interoperability. Currently, the FCC is considering proposals to require the use of more efficient technology on the interoperability channels by 2014.
SPECTRUM EFFICIENCY			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Refarming WT Dkt. No. 99-87 PR Dkt. No. 92-235	"Refarming" is the informal name of various rule-making proceedings initiated in the early 1990s to develop an overall strategy for using the private land mobile radio (PLMR) bands more efficiently so as to meet future communications requirements. These actions affect PLMR spectrum below 800 MHz, including that allocated for public safety use.	The refarming proceedings modified technical standards and operating conditions for public safety operations in the Public Safety Pool, allowing for the development of more advanced and efficient public safety services.	In 2003, the FCC finalized plans to require existing users to migrate from the existing 25 kHz standard technology used in these bands to 12.5 kHz technologies by 2013. Further proceedings are pending to determine whether an additional mandated requirement to 6.25 kHz technologies is necessary.



SPECTRUM EFFICIENCY (cont.)			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
800 MHz Rebanding WT Dkt. No. 02-55	Public safety and CMRS providers (principally Nextel) operate in the 800 MHz band on adjacent frequencies. Due to technical incompatibilities, this channeling plan resulted in interference to public safety systems. In August of 2004, the FCC adopted a resolution that requires Nextel to surrender some of its 800 MHz spectrum and fund the relocation of public safety and other incumbents to new frequency assignments in the 800 MHz band. In exchange, the FCC issued Nextel a license for ten MHz of spectrum in the 1.9 GHz PCS band.	The 800 MHz rebanding project allows public safety users to operate without continuing interference problems. It should also provide additional 800 MHz channel capacity in most markets for public safety communications.	The rebanding process is being implemented by an independent Transition Administrator comprised of BearingPoint, Squire-Sanders-Dempsey LLP, and Baseline Telecom, Inc. The process began on June 27, 2005, and is required to be completed by June 26, 2008.
SPECTRUM NEEDS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Spectrum Needs of Emergency Responders WT Dkt. No. 05-157	The Intelligence Reform Act (Signed December 2004 by President Bush) requires the FCC, in consultation with the Secretary of Homeland Security and the National Telecommunications and Information Administration (NTIA), to assess the short- and long-term spectrum needs of emergency response providers and to report to Congress by December 17, 2005.	The study will provide relevant input to Congress, which may consider providing additional spectrum to promote interoperable communications between local, state, and federal public safety agencies.	In April 2005, the FCC solicited public comment on the need for, operation of, and administration of a nationwide interoperable broadband mobile communications network. The FCC staff is now considering these submissions in order to prepare its report to Congress.



SPECTRUM			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Advanced Wireless Services WT Dkt. No. 05-211 WT Dkt. No. 04-356 WT Dkt. No. 02-353 ET Dkt. No. 00-258 WT Dkt. No. 02-8	<p>The FCC has made spectrum available for new advanced wireless services (AWS), including third generation wireless (3G) mobile broadband. These systems are intended to provide access to a wide range of telecommunication services and other services that are specific to mobile users.</p> <p>In November 2003, the FCC established service rules for the 90 megahertz of AWS spectrum at 1710-1755 and 2110-2155 MHz. Subsequently, the Commission further revised the band plan for this spectrum. The FCC plans to auction this spectrum in June 2006.</p>	NTIA worked with the Department of Defense and other federal agencies to develop a set of proposals to clear the 1.7/2.1 GHz bands for AWS and make certain non-federal bands available for relocating Federal operations. An October 2004 allocation of the 2 GHz and the 2.3 GHz bands allows for the relocation of critical military operations.	<p>In June 2005, the FCC issued a Declaratory Ruling and FNPRM seeking comment on rule changes needed to implement the 2004 Commercial Spectrum Enhancement Act (CSEA), which established a "Spectrum Relocation Fund" to reimburse the relocation costs of federal agencies currently operating on spectrum reallocated from federal to non-federal use. Comments are due August 26, 2005; reply comments are due September 12, 2005.</p> <p>The FCC has indicated its intention to auction the 1.7/2.1 GHz band by mid-year 2006.</p>



SPECTRUM (cont.)			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Wi-Fi/4.9 GHz WT Dkt. No. 00-32	The 4.9 GHz band was transferred from Federal Government to non-Federal Government use in 1999. In 2002, the Commission adopted the fixed and mobile allocation for the band and designated the band for use in support of public safety.	Emergency responders can use the 4.9 GHz band to access the latest broadband technology in support of public safety and homeland security missions, such as wireless local area networks for incident scene management, emergency dispatch operations, and emergency vehicular operations.	In November 2004, the FCC revised its technical specifications for the 4.9 GHz band to allow manufacturers to adapt technologies that are used in adjacent spectrum bands (such as the Unlicensed National Information Infrastructure (U-NII) unlicensed band and the Intelligent Transportation System (ITS) band) for the 4.9 GHz band. The changes allow public safety licensees to use commercial off-the-shelf technologies available for the U-NII and ITS bands. The FCC also reaffirmed its previous decision not to adopt a technology standard or make regional planning mandatory in the 4.9 GHz band.



SPECTRUM (cont.)			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Ultra Wideband ET Dkt. No. 98-153	<p>Ultra-wideband (UWB) devices use pulse modulation (the modulation and emission of short bursts of energy) over large bandwidths to convey information.</p> <p>In February 2002, the FCC amended Part 15 of its rules to permit the marketing and unlicensed operation of products incorporating UWB technology. This raised concern that harmful interference could be caused to critical safety systems, so the FCC implemented UWB standards and operational restrictions on the use of UWB.</p> <p>In February 2003, the FCC modified its UWB regulations to allow for technologies such as through-wall imaging to be used by law enforcement and emergency rescue personnel.</p>	<p>UWB is designed to provide an improved method for providing radar applications where precise distance resolution is required and for providing covert voice or data communications. UWB devices can be used for precise measurement of distances or locations, for obtaining images of objects buried under ground or behind services, and for short-range high-speed data transmission for broadband access to networks. This technology is intended to assist law enforcement, emergency rescue or firefighter personnel in emergency situations.</p>	<p>In December 2004, the FCC amended its rules to provide greater flexibility for the introduction of new wideband devices and systems. The FCC also issued an FNPRM seeking comment on whether it should provide UWB and other unlicensed devices additional flexibility. Comments were due June 30, 2005; reply comments were due July 20, 2005. This proceeding remains pending.</p>



SPECTRUM (cont.)			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Personal Locator Beacons WT Dkt. No. 99-366	<p>Personal Locator Beacons (PLBs) are small transmitters that send out personalized emergency distress alerts. The National Oceanic and Atmospheric Administration (NOAA) and the Air Force Rescue Coordination Center (AFRCC) monitor the signal. A person can obtain an FCC certified PLB without a license, but may not modify it; an FCC certified device has an identifying label placed on it by the manufacturer. When a customer buys a PLB, he or she must register the device with NOAA via mail, fax, or the internet.</p> <p>On July 1, 2003, the FCC authorized the use of PLBs in the 406 MHz band – an internationally recognized distress frequency. The system is an international program to which 36 nations belong.</p>	PLBs are a form of emergency alert and safety communications that provide the general public with a distress and alerting capacity for use in life-threatening situations in remote environments after all other means of notifying search and rescue responders (e.g., telephone, radio) have been exhausted.	No pending proceeding.
NETWORK SECURITY AND RELIABILITY			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Outage Reporting ET Dkt. No. 04-35	All voice/paging communications providers (cable, satellite, wireless, wireline) must comply with the FCC's mandatory network outage reporting requirements. The requirements include simplified criteria for reporting outages that potentially affect 911/E911 as well as special offices and facilities.	Communications providers must fill out standard forms whenever they experience network outages or disruptions of certain magnitudes. These reports are intended to help the industry evaluate network and infrastructure weaknesses.	<p>Seven petitions for reconsideration and/or clarification remain pending.</p> <p>Outage reports are exempted from FOIA requests.</p>



NETWORK SECURITY AND RELIABILITY (cont.)

Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Foreign Ownership Limits IB Dkt. No. 05-55	<p>Many foreign companies invest in U.S. companies that hold FCC licenses. The FCC reviews foreign ownership in FCC radio licenses, and thus foreign ownership in many U.S. communications companies.</p> <p>Section 310(b) of the Communications Act limits the level of foreign ownership in U.S. communications companies. In particular, Section 310(b)(4) establishes a 25% benchmark for investment by foreign individuals, corporations or governments in entities that control a U.S. broadcast, common carrier or radio station license. This section grants the FCC discretion to allow higher levels of foreign ownership unless such ownership is inconsistent with the public interest.</p> <p>In November 2004, the FCC issued Foreign Ownership Guidelines to assist the public and applicants in understanding and complying with the FCC's interpretation of § 310. Seemingly contrary to past precedent, these guidelines extended the 20 percent direct foreign ownership cap for a license to non-controlling, indirect foreign investment in a licensee.</p>	<p>In analyzing whether allowing foreign ownership is in the public interest, the FCC takes into account and affords deference to the Executive Branch agencies on national security, law enforcement, foreign policy, and trade policy issues.</p>	<p>In December 2004, a Petition for Reconsideration of the guidelines was filed with the FCC, contending that the guidelines establish a new approach to minority indirect investment and therefore require a rulemaking. The petition requested that the International Bureau revise the guidelines to reflect the FCC's current practice of permitting foreign investment up to 100% in a U.S. company that owns an indirect, non-controlling interest in an FCC license.</p> <p>Comments and reply comments were due in March 2005. This petition remains pending.</p>



NETWORK SECURITY AND RELIABILITY (cont.)

Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Media Security and Reliability Council (MSRC)	<p>The Media Security and Reliability Council (MSRC) is a Federal Advisory Committee that was formed to study, develop, and report on the reliability, robustness, and security of the broadcast and multichannel video programming distribution (MVPD) industries in emergency situations.</p> <p>The MSRC is comprised of leaders of mass media companies, cable television and satellite service providers, trade associations, public safety representatives, manufacturers, and other related entities.</p>	<p>The MSRC provides recommendations to the FCC and the media industry. Its mission includes preparing a comprehensive national strategy for securing and sustaining broadcast and MVPD facilities throughout the U.S. during terrorist attacks, natural disasters, and all other threats or attacks nationwide.</p>	<p>The MSRC's initial two-year charter culminated in late 2003 with the adoption of 49 recommended best practices for the media industry to improve its safety and prepare for rebuilding in case of an emergency.</p> <p>The MSRC was rechartered in 2004 as MSRC II. The MSRC's two main committees are the Communications Infrastructure Security, Access and Restoration Committee, and the Public Communications and Safety Committee.</p> <p>The MSRC met on Thursday, June 2, 2005 to review progress reports from the Toolkit Development Working Group and the Local Coordination Working Group.</p>
Network Reliability and Interoperability Council (NRIC)	<p>The FCC established NRIC to bring together leaders of the telecommunications industry and telecommunications experts from academic, consumer, and other organizations to explore and recommend measures that will enhance network reliability and security.</p> <p>NRIC partners with the FCC, the communications industry, and public safety to facilitate enhancement of emergency communications networks, homeland security, and best practices across the telecommunications industry. The Council's tasks include facilitating the reliability, robustness, security, and interoperability of communications networks, including emergency communications networks.</p>	<p>The Council makes recommendations to help ensure (1) the security and sustainability of communications networks throughout the U.S., (2) the availability of adequate communications emergencies, and (3) the rapid restoration of communication services in the event of major disruptions.</p>	<p>NRIC held a meeting Tuesday, March 29, 2005 at the FCC. The next meetings are scheduled for Wednesday, September 21, 2005 and Tuesday, December 6, 2005.</p> <p>NRIC's current focus groups examine E911, Homeland Security, Network Best Practices, and Broadband.</p>



E911			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Wireless E911 Phase II Deadline CC Dkt. No. 94-102	<p>The FCC's Enhanced 911 (E911) rules require wireless carriers to provide certain identification information for 911 calls.</p> <p>The new rules have a two-phased approach for network-based and handset-based location technologies.</p> <p>Phase I required carriers to report the telephone number of a wireless 911 caller and the location of the antenna that received the call.</p> <p>Phase II, which began October 2001, requires wireless carriers to provide more precise location information. A major deadline for Phase II is December 31, 2005.</p>	<p>The wireless E911 rules were designed to improve the effectiveness and reliability of wireless 911 service by providing 911 dispatchers with additional information on wireless 911 calls. The FCC rules require wireless carriers to modify network and/or handset technology to comply with these requirements.</p>	<p>By December 31, 2005, carriers must achieve 95% penetration of location-capable handsets among their subscribers.</p> <p>In March 2005, the FCC granted limited waivers of the Phase II rules for some carriers.</p> <p>Depending on the technology employed, the carrier must identify the location of the caller within certain accuracy and reliability standards. The standards for Phase II location accuracy and reliability are as follows: (1) for network-based technologies, 100 meters for 67 percent of calls, and 300 meters for 95 percent of calls, and (2) for handset-based technologies, 50 meters for 67 percent of calls, and 150 meters for 95 percent of calls. In March 2005, NRIC's E911 Focus Group published a report recommending that FCC accuracy rules be measured at the state level.</p>



E911 (cont.)			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
VoIP E911 Requirements WC Dkt. No. 04-36 WC Dkt. No. 05-196	<p>Interconnected VoIP providers must supply enhanced 911 (E911) capabilities as a standard feature to all of their customers from wherever the customer is using the service. All interconnected VoIP 911 calls must be routed through the Wireline E911 Network, a dedicated, redundant, highly reliable wireline network that is interconnected with, but largely separate from, the public switched telephone network (PSTN). Currently providers can rely on the customer to self-report his or her location.</p> <p>In addition, VoIP providers must transmit all 911 calls, call back numbers, and the caller's registered location to designated Public Safety Answering Points (PSAPs) by November 28, 2005. VoIP providers must submit a letter to the FCC detailing compliance with FCC rules by November 28, 2005.</p>	<p>This initiative extended E911 to Internet-enabled services. VoIP providers will have to work with incumbent and competitive LECs to connect to the wireline network to achieve compliance with the E911 requirements.</p>	<p>The FCC created a federal-state task force on VoIP Enhanced 911 (E911) enforcement, staffed by the FCC and State Public Utility Commissions.</p> <p>The FCC extended its initial deadline requiring VoIP providers to obtain affirmative acknowledgements from 100% of their subscribers that they have read and understood an advisory concerning the limitations of their E911 service through August 30, 2005. To receive the extension, the provider must have filed a report with the FCC by August 10, 2005, detailing what actions the provider has taken to advise its subscribers, what percentage of subscribers have submitted an affirmative acknowledgement, and whether/how the provider has distributed warning stickers/labels to all subscribers.</p> <p>In May 2005, the FCC released an NPRM seeking comment on additional solutions to ensure that VoIP providers that interconnect with the nation's PSTN provide reliable E911 service. Comments were due August 15, 2005 and reply comments are due September 12, 2005.</p>



PRIORITY ACCESS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Priority Access Service WT Dkt. No. 05-212 WT Dkt. No. 01-333 WT Dkt. No. 96-86	<p>Priority Access Service (PAS) allows National Security and Emergency Preparedness (NSEP) users, such as national security officials, emergency responders, and those in critical infrastructure industries, to gain access to the next available channel to originate calls during emergencies.</p> <p>The FCC assigned the Office of the Manager of the National Communications System (OMNCS) responsibility for the day-to-day administration of PAS. PAS exists in the wireline public switched telephone network via the Government Emergency Telecommunications Service (GETS) program.</p> <p>Wireless Priority Access (WPS) is an enhancement to basic cellular service that allows NSEP calls to queue for the next available radio channel during an emergency. When used with GETS, WPS will provide priority handling from the origination of the call, through the wireless networks, through the IXC and/or LEC wireline networks, and to the wireless or wireline destination. WPS does not preempt calls or deny public use of the radio spectrum.</p> <p>The National Communications System (NCS) oversees day-to-day aspects of the WPS program, with oversight by the FCC.</p>	<p>Communications common carriers must provide PAS.</p> <p>CMRS providers can voluntarily offer PAS in accordance with policies and procedures set forth in Appendix B to Part 64 of FCC Rules. WPS is provided or will soon be provided nationwide by most wireless providers.</p>	<p>Currently, there are 11,500 WPS users. NCS hopes to provide WPS to 350,000 NSEP users.</p>



EMERGENCY ALERTING			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Amber Alerts/Amber Plan	<p>Amber stands for America's Missing: Broadcast Emergency Response.</p> <p>Under the AMBER Plan, once police confirm a missing child report, an alert is sent to radio and television stations and cable companies. Broadcasters interrupt programming to broadcast information concerning a serious child abduction case using the Emergency Alert System (EAS). To maintain the integrity of the EAS and prevent its overuse, AMBER alerts are used only for the most serious child abduction cases, where police believe the child is in danger of serious bodily harm or death. In 2002, the FCC added a Child Abduction Emergency event code to protect the integrity and credibility of both the AMBER Plan and the EAS system. See below for more information on EAS.</p>	The AMBER Plan uses broadcast communication systems and the EAS to aid the rescue of missing children kidnapped by strangers.	<p>The Wireless AMBER Alerts Initiative is a voluntary partnership between the wireless industry, law-enforcement agencies, and the National Center for Missing & Exploited Children (NCMEC) to distribute AMBER Alerts to wireless subscribers who opt in to receive the messages and are able to receive text messages on their wireless devices.</p> <p>Most national and regional carriers now provide Amber Alerts via text messaging to cell phones, pagers, and PDAs. Wireless subscribers can sign up on various websites or with their cellular telephone carriers to receive this service.</p>
Emergency Alert System EB Dkt. No. 04-296 EB Dkt. No. 04-51	The EAS allows broadcast stations, cable systems, participating satellite companies, and other services to send/receive emergency alerts quickly and automatically. The FCC developed EAS in cooperation with the National Weather Service and the Federal Emergency Management Agency (FEMA). Participation in national EAS alerts is mandatory, whereas participation in state and local area EAS activations is voluntary. The FCC has adopted rules for EAS regarding the technical and operational requirements of EAS. The FCC also ensures that state and local EAS plans conform with FCC rules and regulations. EAS was designed so that if one link breaks down, the entire system does not fail. EAS automatically converts to whatever language the broadcast or cable station uses.	EAS uses digital technology to distribute messages and allows broadcast stations, cable systems, and other services to send and receive emergency information quickly and automatically.	<p>In February 2005, the FCC issued an Order that amended EAS rules to enable wireless cable TV systems to provide EAS alerts to subscribers more efficiently by installing equipment that provides a means to switch all programmed channels to a predesignated channel that carries EAS, instead of installing an EAS decoder for each and every system channel.</p> <p>In an August 2004 NPRM, the FCC sought comment on how EAS can be improved to be more efficient. The action stemmed in part from a recommendation from the MSRC. This proceeding remains pending.</p>



WIRETAPPING			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
CALEA ET Dkt. No. 04-295	<p>Congress enacted the Communications Assistance for Law Enforcement in 1994. This law requires telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization. CALEA applies to all telecommunications carriers as defined by Section 102(8) of CALEA, including all entities engaged in the transmission or switching of wire or electronic communications as a common carrier for hire. A telecommunications carrier must ensure that its equipment, facilities, and services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of meeting the assistance capability requirements.</p>	<p>CALEA preserves the ability of law enforcement to conduct electronic surveillance in the face of rapid advances in telecommunications technology.</p>	<p>In an August 2005 Order, the FCC found that the definition of “telecommunications carrier” in CALEA is broader than the definition of that term in the Communications Act and can encompass providers of services that are not classified as telecommunications services under the Communications Act. As a result, the FCC concluded that facilities-based broadband Internet access service providers and VoIP providers that offer services permitting users to receive calls from, and place calls to, the public switched telephone network must be prepared to accommodate law enforcement wiretaps within 18 months of the effective date of the Order. As of the date of this printing, the text of this Order had not been released.</p> <p>In an August 2004 Declaratory Ruling, the FCC clarified that CMRS carriers offerings of push-to-talk dispatch-like service that are offered in conjunction with interconnected service to the PSTN, but may use different technologies, are subject to CALEA requirements.</p> <p>Whether satellite broadband providers are subject to CALEA requirements remains in dispute.</p>



INTELLIGENT TRANSPORTATION SYSTEMS

Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Short Range Communications - 5.9 GHz WT Dkt. No. 01-90	<p>In December 2003, the FCC established licensing and service rules for the Dedicated Short Range Communications (DSRC) Service in the Intelligent Transportation Systems (ITS) Radio Service in the 5.850-5.925 GHz band (5.9 GHz band). DSRC facilitates the use of radio-based technologies to improve traffic flow and traffic safety.</p> <p>DSRC provides the critical communications link for intelligent transportation systems, which according to the Secretary of Transportation, are the key to achieving the Department of Transportation's (DOT) number one priority of reducing highway fatalities.</p> <p>The 5.9 GHz band is also eligible for use by non-public safety entities for commercial or private DSRC operations.</p>	<p>The DSRC Service involves vehicle-to-vehicle and vehicle-to-infrastructure communications, helping to protect the traveling public. The DSRC messages warn drivers of impending dangerous conditions or events in time to take corrective or evasive actions.</p>	<p>The FCC licenses DSRC Roadside Units (RSUs) and requires licensees to register RSUs by site and segments. Approved applicants are granted non-exclusive licenses for the area requested and operation may not begin until licensees register RSU sites, channels, and data. RSUs at locations within 75 kilometers of Government radar sites are subject to NTIA coordination. On-Board Units mounted in vehicles and portable units are licensed by Part 95 of the FCC Rules.</p> <p>In September 2004, the FCC announced the details of the registration process for the DSRC service and began accepting applications for RSU area licenses and permitting DSRC licensees to register individual transmitter locations starting October 1, 2004.</p>



TECHNOLOGY DEVELOPMENT			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Radio Frequency Identification (RFID) ET Dkt. No. 01-278	<p>RFIDs use radio frequency waves to automatically identify, track, or locate people or objects by transferring data between a movable object and a reader. An RFID system consists of a tag mounted on an item to be identified and a device that receives information transmitted from the tag.</p> <p>The FCC regulates RFID under its Part 15 rules for low-power devices. RFID devices are unlicensed, but the FCC requires that the devices meet radio frequency (RF) emissions limitations, power restrictions, and other requirements before they may be operated or marketed.</p>	<p>The U.S. government is testing RFID technology as a means to quickly and accurately identify visitors at U.S. ports of entry, as part of the DHS's US-VISIT program.</p> <p>RFID can be used to track almost anything, and companies are looking to use RFID to track goods within their supply chain and for other applications.</p>	<p>In April 2004, the FCC authorized the use of RFID with commercial shipping containers so shippers could rapidly inventory contents of containers and could determine whether tampering occurred during shipping. The FCC also increased the maximum signal level permitted for RFID systems operating in the 433.5-434.5 MHz band to facilitate more reliable transmissions with greater range.</p> <p>In October 2004, the FCC held an RFID Workshop to identify regulatory issues for system technologies and deployments.</p> <p>In December 2004, the FCC certified an RFID tracking system that used UWB RFID technology.</p>



AIRPLANE COMMUNICATIONS			
Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Airborne Cellular Use WT Dkt. No. 04-435	<p>FCC rules currently ban cell phone use after a plane has taken off because of potential interference to cellular phone networks on the ground.</p> <p>In addition, the Federal Aviation Administration (FAA) has rules prohibiting in-flight cell phone use because of potential interference to navigation and aircraft systems.</p> <p>The FCC is considering proposals that may allow use of cellular phones or wireless data devices on airplanes after take off. Proposed rule changes are aimed at increasing the communication options for wireless users while ensuring there is no increased risk of harmful interference to cellular systems on the ground.</p>	<p>This proposal would increase the communications options available to public safety and persons on airborne aircraft during emergency situations. Concerns, however, have also been raised regarding the increased ability of terrorists to communicate and coordinate attacks while onboard aircraft.</p>	<p>In Feb. 2005, the FCC proposed to permit airborne operation of wireless handsets, including those used for broadband, as long as such devices operate at the lowest power setting under control of a “pico cell,” a small cellular base station installed onboard the aircraft, and do not interfere with terrestrial cellular systems. Comments were due May 26, 2005; reply comments were due August 11, 2005.</p> <p>Use of personal electronic devices, including all phones and other portable electronic devices (<i>i.e.</i>, pagers, blackberries, portable music players, video games, computers) will remain subject to the FAA’s authority.</p>
Air-Ground Services WT Dkt. No. 03-103 WT Dkt. No. 05-42	<p>Air-ground radiotelephone service allows CMRS providers to offer two-way voice, fax, and data services for hire to subscribers in aircraft, in-flight, or on the ground. The FCC currently licenses these systems by transmitter and site location, so service providers must apply for a license for each and every tower/base site.</p>	<p>Air-ground communications services are provided to federal, state, and local agencies, including the FBI, the U.S. Department of Energy, and the U.S. Customs Service. The air-ground spectrum can also support aircraft management, other public safety services, and homeland security communications.</p>	<p>In early 2005, the FCC adopted an Order reconfiguring the 4 MHz of spectrum in the 800 MHz air-ground band and allowing flexible spectrum access by auctioning new licenses for this spectrum in three possible band plan configurations.</p> <p>The FCC will issue a public notice prior to the Commission’s auction of new 800 MHz air-ground spectrum licenses in which it will specify the filing requirements for the plan.</p>



AIRPLANE COMMUNICATIONS (cont.)

Initiative/Proceeding	Description	Relevance to Homeland Security	Status/Notes
Aeronautical Mobile Satellite Service (AMSS) IB Dkt. No. 05-20	<p>AMSS is a mobile service between aeronautical stations and aircraft stations, or between aircraft stations. The service provides two-way communications, including broadband, onboard an aircraft.</p> <p>The services, including certain frequency bands and technical standards used for this service, are coordinated internationally through the International Civil Aviation Organization to ensure the worldwide interoperability.</p>	<p>Many of the communications within this service are used for air traffic services and aeronautical operational control safety communications.</p> <p>Broadband capability for crews is intended to enhance aircraft operations through real-time equipment and supply information, weather updates, and security monitoring.</p>	<p>In February 2005, the FCC released an NPRM proposing a regulatory scheme for AMSS to communicate with fixed-satellite service networks in the “Ku-Band” (at frequencies in the 11.7-12.2 GHz and 14.0-14.5 GHz Bands). The proposal includes broadband service on aircraft. This proceeding remains pending.</p> <p>In July 2005, law enforcement agencies (DOJ, FBI, Dept. of Homeland Security) submitted comments in response to the NPRM asking the FCC to add in-flight satellite broadband to technologies covered by CALEA.</p>



U.S. Department of Commerce

INTEROPERABILITY			
Initiative	Description	Relevance to Communications	Status/Notes
Presidential Determination: Improving Spectrum Management for the 21st Century	<p>The Determination directs DOC to complete the following tasks related to homeland security:</p> <ol style="list-style-type: none">1) Integrate agency-specific spectrum plans (including the DHS' Spectrum Needs Plan) into a Federal Strategic Spectrum Plan and assist in formulating the National Strategic Spectrum Plan. (Due May 30, 2006).2) Develop a plan for implementing incentives that promote efficient use of spectrum while protecting homeland security. (Due November 30, 2005).3) Establish a plan to implement the recommendations from the June 2004 two-part series of DOC reports entitled "Spectrum Policy for the 21st Century - The Presidents Spectrum Policy Initiative" (Reports). (Due May 30, 2005).4) Provide the President with an annual report that describes the implementation efforts for the recommendations in the Reports. The DHS will prepare a section for this report that describes the progress made with respect to public safety spectrum issues. (Due November 30, 2005, and annually thereafter).	<p>This Determination requires the DOC to evaluate how to distribute and use spectrum for public safety purposes.</p>	<p>The Determination was released November 30, 2004.</p> <p>The plans and reports developed by the DOC will be submitted to the President.</p>



U.S. Department of Agriculture

RURAL DEVELOPMENT			
Initiative	Description	Relevance to Communications	Status/Notes
Rural Information Center (RIC)	The Rural Information Center provides information and referral services to local, tribal, state, and federal government officials; as well as community organizations, rural electric and telephone cooperatives, libraries, businesses, and citizens working to maintain the vitality of America's rural areas.	RIC provides information to rural electric and telephone cooperatives. RIC also provides resources for communications interoperability and emergency preparedness.	Nothing pending.



U.S. Department of Health and Human Services

EMERGENCY RESPONSE			
Initiative	Description	Relevance to Communications	Status/Notes
The Emergency Preparedness Resource Inventory (EPRI)	EPRI is a web-based tool allowing local or regional planners to assemble customized inventories of critical resources that would be useful in responding to a bioterrorist attack, including health care and emergency resources.	The tool uses the internet so communities can assess their regional supply of critical resources, prepare for incident response, estimate gaps, support future resource investment decisions, and help first responders figure out where emergency equipment and medicines are located, how much is available, and whom to contact to obtain those resources.	Released by HHS' Agency for Healthcare Research and Quality.
Report: Altered Standards of Care in Mass Casualty Events	This report offers a framework for how to provide optimal care during a potential bioterrorism or other public health emergency involving thousands, or even tens of thousands, of victims. The report includes the recommendations of a 39-member panel of experts in bioethics, emergency medicine, emergency management, health administration, health law and policy, and public health that was convened in August 2004.	In addition to examining the reallocation of health and medical resources among hospitals and other health facilities, the report considers a number of important non-medical issues, including what public communication strategies are needed before, during, and after a mass casualty event.	HHS' Agency for Healthcare Research and Quality and Office of Public Health Emergency Preparedness convened the panel.



EMERGENCY RESPONSE (cont.)			
Initiative	Description	Relevance to Communications	Status/Notes
New Emergency Information Center Model	<p>This operations model for emergency call centers is designed to help public health agencies and other first responders prepare to provide accurate, timely information during a health emergency.</p> <p>The model is also designed to help public health departments, state and local officials and others gear up quickly to answer calls from the public and health care providers if an emergency arises.</p>	The model offers guidance to organizations on the requirements, specifications and resources needed to develop a public health emergency contact center that is highly integrated with public health agencies and that can reduce the likelihood of hospitals and health systems being overwhelmed with calls and requests for information.	<p>Released by HHS' Agency for Healthcare Research and Quality.</p> <p>A goal of the model is to develop the capacity to handle 1,000 calls per hour from health care providers or members of the public in addition to delivering regular services.</p>



U.S. Congress

INTEROPERABILITY			
Bill	Description	Relevance to Communications	Status/Notes
The Faster and Smarter Funding for First Responders Act of 2005, H.R. 1544	<p>Does not create a new grant program, but rather reforms the manner in which DHS issues Federal grants in an effort to enhance the ability of States, local governments, regions, Indian tribes, and first responders to prevent, prepare for, respond to, and recover from threatened or actual acts of terrorism. Also establishes a common set of rules for the Department's existing terrorism preparedness grant programs.</p> <p>Designed to expedite the delivery of Federal terrorism preparedness assistance to first responders where it is needed most and, at the same time, end undisciplined homeland security spending.</p>	Lists the purchase of interoperable communications equipment as an acceptable use of federal homeland security grant funds. Also lists "telecommunications" as a category of critical infrastructure to be considered when prioritizing grant requests.	<p>House passed the bill on May 12, 2005, by a vote of 409-10. It was then referred to the Senate Committee on Homeland Security and Government Affairs.</p> <p>President Bush recently appointed the bill's sponsor, Congressman Cox (R-CA), Chairman of the Securities and Exchange Commission.</p> <p>Companion Bill – S. 1013</p>
The Homeland Security Grant Enhancement Act, S.21	<p>Requires states applying for homeland security grants to devise a 3-year homeland security plan that includes a strategy to provide interoperable communications. Authorizes certain grants to be used for interoperable communication systems.</p> <p>Establishes an International Border Community Interoperable Communications Demonstration Project.</p>	Makes the interoperability of communications a focus of federal homeland security grants.	<p>Senator Collins (R-ME) introduced this bill on January 25, 2005; the Senate Committee on Homeland Security and Governmental Affairs reported the bill to the full Senate on May 24, 2005. It was then placed on the Senate Legislative Calendar.</p> <p>Senator Collins is the Chair of the Homeland Security and Government Affairs Committee.</p>
The Transportation Security Improvement Act, S. 1052	Directs DHS to establish a program for awarding grants to private operators of over-the-road buses for the installation and/or upgrading of an emergency communications system linking operational headquarters, over-the-road buses, law enforcement, and emergency personnel. § 401	Includes emergency communications systems among priorities for transportation security dollars.	<p>Senator Stevens (R-AK) introduced the bill on May 17, 2005, it was referred to Senate Committee on Commerce, Science, and Transportation.</p> <p>Senator Stevens is the Chairman of the Senate Commerce Committee.</p>



INTEROPERABILITY (cont.)			
Bill	Description	Relevance to Communications	Status/Notes
The Public Safety Interoperability Implementation Act, H.R. 1323	<p>Establishes a Public Safety Communications Trust Fund. Authorizes \$500 million and devotes 50% of the proceeds of certain spectrum auctions to the fund.</p> <p>Grants issued from the Fund would be used to implement interoperability and modernization for the communications needs of public safety, fire, emergency, law enforcement, and crisis management functions of State and local agencies and nonprofit organizations.</p>	Uses spectrum auction funds as a revenue source, and provides grants to improve interoperability.	Congressman Stupak (D-MI) introduced the bill on March 15, 2005, it was then referred to the House Committee on Energy and Commerce.
The Connecting the Operations of National Networks of Emergency Communications Technologies for First Responders Act, H.R. 1251	<p>Directs DHS to develop a national strategy to achieve communications interoperability. Also establishes a grant program for DHS to provide grants to states, local governments, and public safety agencies to achieve communications interoperability.</p> <p>Authorizes \$500 million for FY06, \$750 million for FY07, \$1 billion for FY08, \$1.25 billion for FY09, \$1.5 billion for FY10, and such sums as are necessary each fiscal year thereafter.</p>	Focuses grants on communications interoperability.	Congresswoman Lowey (D-NY) introduced the bill on March 10, 2005, it was then referred to the House Committees on Energy and Commerce and Homeland Security.
The Targeting Terrorist More Effectively Act, S.12	Provides grants to improve police communications through the use of wireless communications, computers, software, etc. so law enforcement agencies will be able to communicate more effectively across jurisdictional boundaries.	Includes emergency communications systems among priorities for rail transportation security dollars.	<p>Senator Biden (D-DE) introduced the bill on January 24, 2005, it was then referred to the Senate Committee on Foreign Relations.</p> <p>Senator Biden, the sponsor of the bill, is the Ranking Member of the committee of jurisdiction.</p>



INTEROPERABILITY (cont.)			
Bill	Description	Relevance to Communications	Status/Notes
Highway Reauthorization bill, H.R. 3	In several sections throughout the Highway Reauthorization bill, programs to enhance the interoperability of emergency communications systems are made eligible for grants, or are noted as a priority for the receipt of grants.	Includes emergency communications systems among priorities for transportation security dollars.	The Senate and the House passed the bill on July 29 and it was cleared for the White House. President Bush announced that he will veto any highway bill that spends more than \$284 billion.
The Improve Interoperable Communications and First Responders Act, S.1274	Establishes an Office of Interoperability and Compatibility within the Directorate of Science and Technology at DHS. Strengthens Federal leadership, provides grants, enhances outreach and guidance, and provides other support to state and local officials to achieve communications interoperability and foster improved regional collaboration and coordination.	Makes communications interoperability among first responders a priority at DHS.	Senator Lieberman (D-CT) introduced the bill on June 21, 2005, it was then referred to the Senate Committee on Homeland Security and Government Affairs. Senator Lieberman is the Ranking Member of the committee of jurisdiction. Senator Collins, the Chair of the Committee, is a co-sponsor.
DHS Authorization Act for FY 2006, H.R. 1817	Authorizes \$2 billion in grants for state and local government terrorism preparedness. Calls on the Office for Interoperability and Compatibility to focus on a comprehensive national approach to achieving interoperable communications. §§ 107, 308	Ensures that technical assistance and grant guidance will be available so first responders can achieve interoperable communications.	Passed the House May 18, 2005 by 424-4. Referred to Senate Committee on Homeland Security and Governmental Affairs on May 19, 2005. President Bush recently appointed the bill's sponsor, Congressman Cox, to be Chairman of the SEC.

INTEROPERABILITY (cont.)			
Bill	Description	Relevance to Communications	Status/Notes
The Domestic Defense Fund Act, S. 140	<p>Authorizes DHS to award grants to states, local governments, and Indian tribes for the development and maintenance of communications systems that can be used between and among first responders, including law enforcement, fire, and emergency medical personnel.</p> <p>Authorizes \$1 billion for each of the fiscal years 2006 through 2009 for State and Regional Planning and Communication Systems.</p>	Provides grants to improve the interoperability of first responder communications.	Senators Clinton (D-NY) and Schumer (D-NY) introduced the bill on January 24, 2005, it was then referred to Senate Committee on Homeland Security and Governmental Affairs.
The Smarter Funding for All of America's Homeland Security Act, H.R. 91	Directs DHS to establish a State and Regional First Responder Grant Program. Grants would go to states and eligible regional entities for, among other things, threats to major communications nodes including cyber and telephonic nodes.	Provides grants to protect against threats to telecommunications systems.	Congressman Frelinghuysen (R-NJ) introduced the bill on March 10, 2005, it was then referred to the House Committees on Homeland Security and Energy and Commerce.
DHS Appropriations Act, H.R. 2360	Both the House and the Senate committee reports contain money to fund grants to enhance interoperability between various first responders.		Congressman Rogers (R-KY) introduced the bill. It passed the House on May 17 by a vote of 424-1. It passed the Senate on July 14. The Senate has appointed conferees. The House will appoint conferees after recess.
SPECTRUM			
Bill	Description	Relevance to Communications	Status/Notes
The Homeland Emergency Response Operations (HERO) Act, H.R. 1646	Makes dedicated analog spectrum between 764 and 776 megahertz, inclusive, and between 794 and 806 megahertz, inclusive, available for emergency communications.	Provides spectrum for emergency communications.	Congresswoman Harmon (D-CA) introduced the bill on April 14, 2005, it was referred to the House Committee on Energy and Commerce on April 15 2005.



SPECTRUM (cont.)			
Bill	Description	Relevance to Communications	Status/Notes
The SAVE LIVES Act, S. 1268	Sets a specific date for the availability of spectrum for public safety organizations and creates a deadline for the transition to digital television.	Provides spectrum for emergency communications.	Senators McCain (R-AZ) and Lieberman (D-CT) introduced the bill on June 20, 2005, it was then referred to the Senate Committee on Commerce, Science and Transportation. S.1237, a bill with the same title, was introduced by the same two Senators on June 14, 2005.
NETWORK SECURITY AND RELIABILITY			
Bill	Description	Relevance to Communications	Status/Notes
Rail Transit Security and Safety Act, H.R. 1109	<p>Directs DHS and DOT to complete a vulnerability assessment of freight and passenger rail transportation, including the communications systems utilized for freight and rail transportation.</p> <p>Authorizes DHS to award grants to public transportation agencies for capital security improvements, including the purchase of communications equipment.</p> <p>Authorizes DOT to award grants to Amtrak for tunnel improvement, including the installation of emergency communications and lighting systems.</p>	Includes emergency communications systems among priorities for rail transportation security dollars.	<p>Congressman Lynch (D-MA) introduced the bill on March 3, 2005, it was then referred to the House Committee on Homeland Security and the House Committee on Transportation and Infrastructure.</p> <p>Companion Bills: H.R. 153, H.R. 2351</p> <p><i>See also</i> certain provisions of S.12.</p> <p><i>See also</i> The Transportation Security Improvement Act, S. 1052, Introduced May 17, 2005 by Senator Stevens. Referred to the Senate Committee on Commerce, Science, and Transportation.</p>



E911			
Bill	Description	Relevance to Communications	Status/Notes
The IP-Enabled Voice Communications and Public Safety Act, S.1063	Requires the FCC to prescribe regulations to establish a set of requirements or obligations for providers of IP-enabled voice service to ensure that 911 and E-911 services are available to customers of IP-enabled voice service.	Focuses on E-911 and VoIP.	Senators Nelson (D-FL), Burns (R-MT), and Clinton (D-NY) introduced the bill on May 18, 2005, it was then referred to the Senate Committee on Commerce, Science and Transportation. An identical bill – H.R. 2418 – was introduced by Congressman Bart Gordon (D-TN) on May 18, 2005. That bill was referred to the House Committee on Energy and Commerce.
EMERGENCY ALERT			
Bill	Description	Relevance to Communications	Status/Notes
The Transportation Security Improvement Act, S. 1052	Directs DHS to develop a national response system that will allow the public sector to receive security alerts, emergency messages regarding hazardous material accidents, threats, thefts, or other safety and security risks or incidents. § 409	Focuses on emergency communications.	Senator Stevens (R-AK) introduced the bill on May 17, 2005, it was then referred to the Senate Committee on Commerce, Science, and Transportation. Senator Stevens is the Chairman of the committee of jurisdiction.
The Extremely Hazardous Materials Transportation Security Act, H.R. 1414	Directs DHS to promulgate rules to ensure effective and immediate communication between transporters of extremely hazardous materials and all entities charged with responding to acts of terrorism involving shipments of extremely hazardous materials.	Focuses on emergency communications.	Congressman Markey (D-MA) introduced the bill on March 17, 2005, it was then referred to the House Committees on Homeland Security and Transportation and Infrastructure.



TECHNOLOGY DEVELOPMENT			
Bill	Description	Relevance to Communications	Status/Notes
DHS Authorization Act for FY 2006, H.R. 1817	Directs DHS to establish a homeland security technology transfer program that would facilitate the identification, modification, and commercialization of technology equipment for use by Federal, State, and local governmental agencies, emergency response providers, and the private sector to prevent, prepare for, and respond to acts of terrorism. § 302	Requires DHS to focus on threats to major communications nodes.	Passed the House May 18, 2005 by 424-4. Referred to Senate Committee on Homeland Security and Governmental Affairs on May 19, 2005. President Bush recently appointed the bill's sponsor, Congressman Cox, to be Chairman of the SEC.
The Strengthen Aviation Security Act, H.R. 2649	Directs DHS to study the viability of devices to enable discreet, wireless communications between flight attendants, pilots, Federal Air Marshals, and ground-based personnel during a passenger commercial air flight to improve coordination of planning and activities in the event of an act of terrorism.	Focuses on wireless communication between commercial air flights and ground crews.	Congressman Markey (D-MA) introduced the bill on May 26, 2005, it was referred to the House Committees on Homeland Security and the Judiciary the same day.
The 9/11 Can You Hear Me Now Act, H.R. 1794	Directs DHS to develop and provide improved communications equipment, including radios, for the New York City Fire Department.	Provides for improved communications equipment for first responders.	Congresswoman Maloney (D-NY) introduced the bill on April 21, 2005, it was then referred to the House Committee on Energy and Commerce.
The Transportation Security Improvement Act, S. 1052	Requires certain trucks carrying hazardous materials to install wireless or satellite communications technology that provides communications, vehicle position location, tracking capabilities, and emergency messages. § 403	Includes emergency communications systems among priorities for transportation security dollars.	Senator Stevens (R-AK) introduced the bill on May 17, 2005, it was then referred to Senate Committee on Commerce, Science, and Transportation. Senator Stevens is the Chairman of that Committee.



Wiley Rein & Fielding LLP

Contact Information

Nancy J. Victory 202.719.7344 nvictory@wrf.com
Michael Lewis 202.719.7338 mlewis@wrf.com
Thomas S. Dombrowsky, Jr. 202.719.7236 tdombrowsky@wrf.com
Catherine M. Hilke 202.719.7418 chilke@wrf.com

Wiley Rein & Fielding LLP
1776 K Street NW
Washington, DC 20006
www.wrf.com